(a) extraction means for extracting angle and distance data relating different parts of the user's signature inputted into the system by the input device;

(b) registration means for setting up a reference data file compiled from angle and distance data relating to a plurality of samples of the user's signature inputted into the system by the user by means of the manual input device during a registration phase;

(c) comparison means for comparing the angle and distance data extracted by the extraction means from the user's signature inputted into the system during an authentication phase to reference angle and distance data held in the reference data file, according to defined verification criteria ; and

(d) verification means for providing an output indicative of an appropriate match between the inputted signature to be authenticated and the reference data in dependence on the result of the comparison, thereby providing verification of the user's signature.

Such a system can provide an on-line dynamic biometric verification system that can be customised to multiple Internet based applications requiring secure authentication. The system requires no specialised equipment at the point of use, allowing access from any Internet capable computer with a mouse and Java compliant browser for example.

In this context it should be appreciated that the term "signature" is used in this specification to denote an electronic representation of an actual signature (the actual signature consisting of a distinctive representation of the user's name or any other distinctive pattern or representation, such as an emblem, mark or pictogram produced by the user), this electronic representation comprising in practice electronic data constituting an abstraction of the actual signature, for example by incorporating extracted angle and distance data relating to the signature as will be described more fully below. Furthermore the term "reference signature" is used to denote an electronic representation of a hypothetical authentic signature to which the inputted signature is to be compared, this hypothetical authentic signature comprising data constituting an

abstraction of the actual signature extracted from a number of samples of the actual signature and possibly varying with time as further examples of the actual signature are sampled.

CLAIMS:

1. An authentication system for authenticating a user's signature as electronically inputted into the system by a manual input device providing an output indicative of its location with respect to time when manipulated by the user, the system comprising:

(a) extraction means for extracting angle and distance data relating different parts of the user's signature inputted into the system by the manual input device;

(b) registration means for setting up a reference data file compiled from angle and distance data relating to a plurality of samples of the user's signature inputted into the system by the user by means of the manual input device during a registration phase;

(c) comparison means for comparing the angle and distance data extracted by the extraction means from the user's signature inputted into the system during an authentication phase to reference angle and distance data held in the reference data file, according to defined verification criteria ; and

(d) verification means for providing an output indicative of an appropriate match between the inputted signature to be authenticated and the reference data in dependence on the result of the comparison, thereby providing verification of the user's signature.

2. A system according to claim 1, wherein the extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating some of said points to other points in the user's signature as inputted into the system by the manual input device.

3. A system according to claim 2, wherein the extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating each of a number of said points to an immediately preceding point in the user's signature as inputted into the system by the manual input device.

4. A system according to claim 2 or 3, wherein the extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating a last point to a first point in the user's signature as inputted into the system by the manual input device.

5. A system according to any preceding claim, wherein the extraction means includes angle extract means for extracting angle data concerning the relative angular positions of a plurality of points of the user's signature.

6. A system according to any preceding claim, wherein the extraction means includes distance extract means for extracting distance data concerning the relative distances apart of a plurality of points of the user's signature.

7. A system according to any preceding claim, wherein the extraction means includes timing extract means for extracting timing data indicative of the relative times between execution of different parts of the user's signature, and the comparison means is adapted to compare the extracted timing data with reference timing data in the reference data file.

8. A system according to any preceding claim, wherein password verification means is provided for verifying input of a required password, as determined by reference password means, by the user using a keyboard input device.

9. A system according to claim 8, wherein timing verification means is provided for verifying input of the password by the user with the required timing, as determined by reference timing means, using the keyboard input device.

10. A system according to claim 9, wherein the timing verification means includes means for verifying the hold times for which the relevant keys of the keyboard input device are depressed during input of the password, and means for verifying the latency

times between the release of one key and the depression of the following key during use of the keyboard input device to enter the password.

11. A system according to any preceding claim, wherein user name input means is provided for receiving a user name inputted into the system to identify the identity of the user for the purposes of selection of the required reference data file for that user.

12. A system according to any preceding claim, wherein the comparison means incorporates at least one neural network for determining the verification criteria by which a match is to be judged.

13. A system according to any preceding claim, wherein the extraction means is adapted to extract data relating to different features of the user's signature selected according to the fitness of such features to discriminate the user's signature for the purposes of verification and determined by a fitness function relating the relative fitness of the features to their form and number.

14. A system according to claim 13, wherein the fitness function is optimised by an optimisation algorithm, such as a genetic algorithm.

15. A system according to any preceding claim, wherein training means is provided for training the system to refine the verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature inputted into the system by the user during the registration phase and generated false samples.

16 A system according to any preceding claim, wherein the verification means is adapted to provide a reject output indicative of non-matching of one or more verification criteria only after completion of all the verification procedures.